UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/747,770	12/22/2000	Ron J. Vandergeest	0500.0008171 (10500.00.81	4395

24228 7590 06/08/2004

MARKISON & RECKAMP, PC
PO BOX 06229
WACKER DR
CHICAGO, IL 60606-0229

EXAMINER	
HO, THOMAS M	

ART UNIT	PAPER NUMBER
2134	4

DATE MAILED: 06/08/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/747,770	VANDERGEEST ET AL.	
	Examiner	Art Unit	
	Thomas M Ho	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on 22 December 2000.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-31 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-31 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on 22 December 2000 is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-31 are pending.

Claim Rejections - 35 USC § 102

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3. Claims 1-31 are rejected under 35 U.S.C. 102(e) as being anticipated by Crane et al.

In reference to claim 1:

Crane et al. discloses a method for providing user authentication comprising:

- sending, by a first unit, user identification data to an authentication unit, where the first unit is the authentication server which contains the user identification data, the authentication unit is the device from which user receives the data. (Column 4, lines 48 – 52)
- using the user identification data to determine which destination unit will receive the authentication code to authenticate the user, where the identification data received is device specific (Column 4, lines 48 –52)

- sending the authentication code to the determined destination unit based on the user identification data, where the data is sent and received by the authentication device of the user (Column 4, lines 48 –52)
- returning the authentication code to the authentication unit, where the authentication code returned is the token. (Column 5 lines 23-37)
- authenticating the user when the returned authentication code matches the sent authentication code, where the device authentication server authenticates the user. (Column 5, lines 28-35)

In reference to claim 2:

Crane et al. (Column 5, lines 35-43) discloses a method including the step of generating the authentication code on a per authentication session basis and sending the authentication code to the determined destination unit in response to the generated authentication code, where authentication code is a token generated on a per session basis through the device id.

In reference to claim 3:

Crane et al. (Column 4, line 58 – Column 5, line 27) discloses a method including the step of maintaining per user destination unit data including at least one destination unit identifier per user[phone number, IP address] and wherein the step of using the user identification data to determine which destination unit will receive the authentication code includes sending the authentication code to the determined destination unit based on the stored per user destination

unit identifier, where the per user destination unit identifier is the device ID, and the data of the user is maintained in a database containing userIDs matched with device IDs.

In reference to claim 4:

Crane et al. (Column 4, line 48 – Column 5, line 36) discloses a method including the step of receiving user input in response to the step of sending the authentication code and waiting to return the authentication code to the authentication unit until receipt of the user input, where after the authentication code is sent out the first time, the user enters in authentication data to be sent off to the server, and where the Authentication code isn't returned until the user gives this input.

In reference to claim 5:

Crane et al. (Column 5, lines 14-43) discloses a method including the steps of:

Prior to returning the authentication code to the authentication unit, digitally signing, by the first unit, the returned authentication code to produce a digitally signed authentication code that was received from the determined destination unit, where the returned authentication code is digitally signed by the device authentication server.

Verifying [by the authentication unit,] the digitally signed authentication code as part of step (e), where the application server processes the digitally signed response.

In reference to claim 9:

Crane et al. (Column 5, lines 14-43) discloses a method wherein the returned authentication code is digitally signed and including the step of verifying, by the authentication unit, the digitally

signed authentication code as part of the step of authenticating the user, based on the returned authentication code when the returned authentication code matches the sent authentication code, where the authentication code is returned only when the device ID and the user ID match with the originally sent authentication data, where the returned authentication code is digitally signed by the device authentication server, and where the application server processes the digitally signed response.

In reference to claim 10:

Crane et al. discloses a method for providing user authentication comprising:

- Sending primary authentication information on a primary wireless channel by a primary authentication information provider to an authentication unit during a session, where the first unit is the authentication server which contains the primary authentication information, the authentication unit is the device from which user receives the data. (Column 4, lines 48 –52)
- Using the primary authentication information to determine which destination unit will receive an authentication code as a secondary authentication information via a wireless back channel to be used to authenticate the user, where the identification data received is device specific in order to determine which destination unit will receive the information, (Column 4, lines 48 –52) and where the secondary authentication information received is understood to be sent through a number of different alternative channels some wireless like token cards or biometric scanners. (Column 3, lines 14-37)

- Sending the authentication code on the wireless back channel to the destination unit based on the primary authentication information during the same session, where it is disclosed that the data is sent to the authentication device associated with the user which may be one of the many supported include wireless devices. (Column 4, lines 48 –52)
- Returning the authentication code on the wireless primary channel to the authentication unit during the same session, where the authentication code is returned in the form of a digital token. (Column 5 lines 23-37)
- Authenticating the user when the returned authentication code received from the wireless primary channel matches the sent authentication code that was sent on the wireless back channel, where the device authentication server authenticates the user (Column 5 lines 28-35)

In reference to claim 15:

Crane et al. (Column 1, lines 25-39) & (Column 6, line 1-14) discloses a method including the step of sending the authentication code on the wireless back channel[or data based on it] to the destination unit using at least one of a short message session(SMS) channel, a paging channel and a control channel, where it is understood that a wide variety of authentication devices is supported such as biometric scanners or token cards which are frequently known in the art to operate based on a RF (radio frequency) transmission.

In reference to claim 16:

Crane et al. (Column 5, lines 14-36) discloses a method including the step of validating the primary authentication information, where the device authentication server validates the primary authentication information.

Claims 17, 6 are rejected for the same reasons as claim 1.

Claims 22, 18, 11, 7 are rejected for the same reasons as claim 2.

Claims 23, 19, 12, 8 are rejected for the same reasons as claim 3.

Claims 24, 13 are rejected for the same reasons as claim 4.

Claims 25, 14 are rejected for the same reasons as claim 5.

Claim 20 is rejected for the same reasons as claim 9.

Claim 21 is rejected for the same reasons as claim 10.

Claim 26 is rejected for the same reasons as claim 15.

In reference to claim 27:

Crane et al. (Column 4, line 48 – Column 5, line 53) discloses a system for providing user authentication comprising:

- A first unit, where the first unit is authentication server containing the database of authentication information.
- A second unit operatively coupleable to the first unit via a primary wireless channel and operatively coupleable to an authenticator, where the second unit is the unit the user first receives data on.

- A third unit, operatively coupleable to the second unit via a wireless back channel, where the third unit may be an alternate authentication device such as a biometric scanner, or a token card reader (Column 5, lines 5-27)
- The first unit operative to send primary authentication information via the primary channel during a session to the second unit, where client receives the primary authentication information from the server on a second unit, where the second unit is user specific. (Column 4, lines 48-52)
- The authenticator operative to use the primary authentication information to determine which destination unit, other that the first unit, will receive an authentication code as a secondary authentication information via the wireless back channel and wherein the destination unit is the third unit, where the authenticator operative to use the primary authentication information is operative in using the userID and the deviceID in order to determine which unit will receive, via wireless back, such as Radio frequency transmission, the secondary authentication information, such as a user specific per session based token such as those well known in the art(Column 5, lines 28-37), and wherein the destination unit is the chosen third unit set by the user through the deviceID set through the transmission of the user authentication information transmitted from said second unit operatively coupled to the first unit, the primary authentication servers. (Column 4, lines 48-52)
- The second unit operative to the send the authentication code on the wireless back channel to the destination unit based on the primary authentication information sent via

the primary channel during the same session, where the information transmitted by the second unit is eventually received at the destination unit. (Column 4, lines 48-52)

- The first unit operative to return the authentication code on the wireless primary channel to the second unit during the same session, where the first unit returns the authentication code to the user device in the first place. (Column 5, lines 23-37)
- The authenticator operative to authenticate the user which the returned authentication code received from the wireless primary channel matches the sent authentication code that was sent on the wireless back channel, where the data is matched by the device authentication server. (Column 5, lines 28-35)

In reference to claim 28:

Crane et al. (Column 4, line 48 – Column line 27) discloses a system wherein the authenticator maintains per user destination unit data including at least one destination unit identifier per user and sends the authentication code to the second unit for transmission to the destination unit based on the stored per user destination unit identifier, where the data stored in the database maintains information such as the deviceID and sends the code to that particular user device used on the userID.

In reference to claim 29:

Crane et al. (Column 4, lines 48 – Column 5, line 36) discloses a system wherein the first unit includes an interface to receive user input in response to the sending of the authentication code

and wherein the first unit waits to return the authentication code for the authenticator until receipt of the user input, where the first unit receives a userID and a device ID.

In reference to claim 30:

Crane et al. (Column 5, lines 14-43) discloses a system wherein the first unit includes a cryptographic engine and prior to the first unit returning the authentication code for the authenticator, digital signs the returned authentication code to produce a digital signed authentication code that was received from the third unit, and wherein the authenticator verifies the digitally signed authentication code as part of authenticating the user, where the returned authentication code is digitally signed by the device authentication server, and where the application server processes the digitally signed response.

In reference to claim 31:

Crane et al. (Column 1, lines 25-39) & (Column 6, line 1-14) discloses a system wherein the second unit send the authentication code on the wireless back channel to the third unit using at least one of: a short message session (SMS) channel, a paging channel and a control channel, where it is understood that a wide variety of authentication devices is supported such as biometric scanners or token cards which are frequently known in the art to operate based on a RF (radio frequency) transmission.

Conclusion

4. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

US patent 5,299,263 discloses a system of authentication between a system of two parties using public key cryptography. It is well known in the art that public key cryptography often involves the collusion of several parties in order to satisfy a single authentication.

US patent 5,280,581 discloses a system of authentication where a user uses a computer and then sends in authentication information. The user then breaks the connection to authenticate again, and the computer returns the authentication information to another external device.

US patent 6,651,168 discloses a system of authentication that maintains a plurality of different sequences for various authentication processes and devices.

5. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thomas M Ho whose telephone number is (703)305-8029. The examiner can normally be reached on M-F from 8:30am – 5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory A. Morse can be reached at (703)308-4789. The fax phone numbers for the organization where this application or proceeding is assigned are (703)746-7239 for regular communications and (703)746-7238 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703)306-5484.

TMH

May 27th 2004

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100